Notice of Allowability	Application No.	Applicant(s)	
	09/381,056	MERTES ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *22 October 2007*.

2. ☒ The allowed claim(s) is/are *4-9*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 1-3 have been cancelled.

2. Claims 4-9 are pending.

Response to Arguments

3. Applicant's arguments filed 22 October 2007 have been fully considered and they are persuasive.

Allowable Subject Matter

4. **Claims 4-9** are allowed.

5. The following is an examiner's statement of reasons for allowance: The present invention is directed towards a method for generating a asymmetrical cryptographic keys by the user. Claim 4 identifies the uniquely distinct features "**generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central, secure location corresponding to a trust center and an operation performed at a user location in cooperation with the trust center using a secure transmission between a user and the trust center, the method comprising the steps of**

causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair;

producing by the user the at least one encryption key pair including a public part and a secret part;

marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair;

after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center;

unequivocally assigning the at least one encryption key pair to the user;

causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair;

after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair;

encrypting the new certificate using the public part of the at least one encryption key pair;

and causing the trust center to transmit the encrypted new certificate to the user".

Claim 7 identifies the uniquely distinct features "**generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central, secure location corresponding to a trust center and an operation performed at a user location in cooperation with the trust center using**

a secure transmission between a user and the trust center, the method comprising the steps of

causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair;

producing by the user the at least one encryption key pair including a public part and a secret part;

marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair;

after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center;

unequivocally assigning the at least one encryption key pair to the user;

causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair;

after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair;

encrypting the new certificate using the public part of the at least one encryption key pair;

causing the trust center to transmit the encrypted new certificate to the user;

in each bilateral communication occurring between a user desiring no communication with the trust center and another user, marking and making available to the other user the public part of the at least one encryption key pair by using the secret part of the previously generated signature key pair;

and checking a correctness of an assignment regarding the public part of the at least one encryption key pair by performing the steps of:

verifying a signature, and checking a genuineness and a validity of the new certificate in the trust center".

The closest prior art, Bathrick et al. (US Patent No. 5,825,300) discloses a computer system and a method for the protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain, including the steps of sending keying material, including a password, generated by the Certifying Authority to the entity via a secure medium; generating and protecting, by the entity, a public and a private key pair using the keying material provided it by the certifying authority; generating, protecting and sending a request for a certificate to the certifying authority using the keying material provided it by the certifying authority; requesting, by the certifying authority, that the public key and address of the entity be sent to the certifying authority; protecting and sending the public key and address of the entity to the certifying authority using the keying material provided it by the certifying authority; assembling and issuing the certificate to the entity from the

certifying authority and recording the public key of the entity at the certifying authority for public use within the domain of the certifying authority.

However, either singularly or in combination, Bathrick et al. fail to anticipate or render the claimed limitation of **causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair; unequivocally assigning the at least one encryption key pair to the user; causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair; after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair; and encrypting the new certificate using the public part of the at least one encryption key pair.**

The closest prior art, Fischer (US Patent No. 4,868,877) discloses a public key cryptographic system is disclosed with enhanced digital signature certification which authenticates the identity of the public key holder. A hierarchy of nested certifications and signatures are employed which indicate the authority and responsibility levels of the individual whose signature is being certified. The present invention enhances the capabilities of public key cryptography so that it may be employed in a wider variety of business transactions, even those where two parties may be virtually unknown to each other. Counter-signature and joint-signature requirements are referenced in each digital

certification to permit business transactions to take place electronically, which heretofore often only would take place after at least one party physically winds his way through a corporate bureaucracy. The certifier in constructing a certificate generates a special message that includes fields identifying the public key which is being certified, and the name of the certifiee. In addition, the certificate constructed by the certifier includes the authority which is being granted including information which reflects issues of concern to the certifier such as, for example, the monetary limit for the certifiee and the level of trust which is granted to the certifiee. The certificate may also specify cosignature requirements which are being imposed upon the certifiee.

However, either singularly or in combination, Fischer fail to anticipate or render the claimed limitation of **causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair; unequivocally assigning the at least one encryption key pair to the user; causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair; after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair; and encrypting the new certificate using the public part of the at least one encryption key pair.**

The closest prior art, Matyas et al. (US Patent No. 5,164,988) discloses a method to establish and enforce a network cryptographic security policy in a public key cryptosystem wherein device A in a public key cryptographic network will be constrained to continue to faithfully practice a security policy dictated by a network certification center, long after device A's public key PUMa has been certified. If device A alters its operations from the limits encoded in its configuration vector, for example by loading a new configuration vector, device A will be denied participation in the network. To accomplish this enforcement of the network security policy dictated by the certification center, it is necessary for the certification center to verify at the time device A requests certification of its public key PUMa, that device A is configured with the currently authorized configuration vector. Device A is required to transmit to the certification center a copy of device A's current configuration vector, in an audit record. the certification center then compares device A's copy of the configuration vector with the authorized configuration vector for device A stored at the certification center. If the comparison is satisfactory, then the certification center will issue the requested certificate and will produce a digital signature dSigPRC on a representation of device A's public key PUMa, using the certification center's private certification key PRC. Thereafter, if device A attempts to change its configuration vector, device A's privacy key PRMa corresponding to the certified public key PUMa, will automatically become unavailable for use in communicating in the network.

However, either singularly or in combination, Matyas et al. fail to anticipate or render the claimed limitation of **causing the trust center to provide the user with a**

previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair; unequivocally assigning the at least one encryption key pair to the user; causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair; after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair; and encrypting the new certificate using the public part of the at least one encryption key pair.

6. Therefore, **claims 4 and 7** and the respective **dependent claims 5-6 and 8-9** are in condition for allowance.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cdf
December 7, 2007

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137